

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) ~~In a system~~ A method for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, ~~[[a]] the method comprising the steps of:~~
 - (a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information, and wherein the public key is associated with the account in a computer database; and thereafter
 - (b) receiving the electronic communication from the sender,
 - (i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account, ~~account in step (a)~~;
 - (ii) wherein the electronic communication comprises,
 - (A) the sender identity information, and
 - (B) a digital signature derived from an electronic message using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message, and
 - (iii) wherein the electronic communication is communicated electronically from the sender; and
 - (c) validating the identity of the sender for the electronic communication by only; ~~only performing the steps of,~~
 - (i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account, ~~account performed in step (a)~~; and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key, whereby a comparison resulting in a match validates the identity of the sender.

2. (Currently Amended) ~~In a system~~ A method for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, ~~[[a]] the method comprising:~~ comprising the steps of:

(a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account, ~~account in step (a)~~,

(ii) wherein the electronic communication comprises,

(A) the sender identity information, and

(B) a digital signature derived from an electronic message using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message, and

(iii) wherein the electronic communication is communicated electronically from the sender; and

(c) validating the identity of the sender for the electronic communication by,

(i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account, ~~account performed in step (a)~~, and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital

signature comprises decrypting the digital signature using the public key, whereby a comparison resulting in a match validates the identity of the sender, and wherein neither a PIN nor a password is required to be transmitted to the receiver for validating the identity of the sender.

3. (Currently Amended) ~~In a system~~ A method for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, ~~[[a]] the method comprising: comprising the steps of:~~

(a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information and the sender identity information comprises other than an account number, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account, ~~account in step (a)~~,

(ii) wherein the electronic communication comprises,

(A) the sender identity information, and

(B) a digital signature derived from an electronic message using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message, and

(iii) wherein the electronic communication is communicated electronically from the sender; and

(c) validating the identity of the sender for the electronic communication by,

(i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account, ~~account performed in step (a)~~, and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital

signature comprises decrypting the digital signature using the public key, whereby a comparison resulting in a match validates the identity of the sender.

4. (Currently Amended) ~~In a system~~ A method for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, ~~[[a]] the method comprising: comprising the steps of:~~

(a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the account comprises entity information, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i) wherein the electronic communication was created after the association of the sender identity information and the public key with the account, ~~account in step (a)~~;

(ii) wherein the electronic communication comprises,

(A) the sender identity information, and

(B) a digital signature derived from an electronic message using the private key of the pair from an electronic message possessed first by the sender before the receiver, the sender identity information being different from the electronic message,

(iii) wherein the electronic communication is communicated electronically from the sender, and (iv) wherein the electronic communication is the only electronic communication received from the sender by the receiver relating to the action; and

(c) validating the identity of the sender for the electronic communication by,

(i) utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account, ~~account performed in step (a)~~; and

(ii) comparing a function of the public key and the digital signature with a function of the electronic message, wherein the function of the public key and the digital signature comprises decrypting the digital signature using the public key, whereby a comparison

resulting in a match validates the identity of the sender.

5. (Original) The method of claims 1, 2, 3, or 4, wherein the electronic communication includes the electronic message.
6. (Original) The method of claims 1, 2, 3, or 4, wherein the electronic message is implied from the receipt of the electronic communication.
7. (Original) The method of claims 1, 2, 3, or 4, wherein the digital signature is derived within a smart card of the sender.
8. (Original) The method of claims 1, 2, 3, or 4, wherein the digital signature is received from the sender within a terminal of a third-party and then forwarded to the receiver.
9. (Original) The method of claims 1, 2, 3, or 4, wherein the electronic communication is received over a secure network.
10. (Original) The method of claims 1, 2, 3, or 4, wherein the electronic communication is received over an insecure network.
11. (Original) The method of claim 10, wherein the network comprises the Internet.
12. (Original) The method of claims 1, 2, 3, or 4, wherein the electronic communication is received encrypted.
13. (Original) The method of claims 1, 2, 3, or 4, wherein the electronic communication is received unencrypted.

14. (Original) The method of claims 1, 2, 3, or 4, wherein the receiver is a financial institution and the action on the account comprises a financial transaction.
15. (Original) The method of claims 1, 2, 3, or 4, wherein the electronic communication includes the public key.
16. (Original) The method of claims 1, 2, or 4, wherein the sender identity information comprises the account number.
17. (Original) The method of claims 1, 2, or 4, wherein the sender identity information comprises other than the account number.
18. (Original) The method of claims 1, 2, 3, or 4, wherein the public key was associated with the account when the account was first established.
19. (Original) The method of claim 18, wherein the public key was provided by the sender to the receiver.
20. (Original) The method of claim 18, wherein the public key was provided to the sender by the receiver.
21. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information includes information required to process the action.
22. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information comprises a personal identification number (PIN).
23. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information comprises

information validated when the account was established.

24. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information comprises information that was validated in a face-to-face acknowledgement between the sender and the receiver.

25. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information comprises the social security number of the sender.

26. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information comprises the address of the sender.

27. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information comprises the mother's maiden name of the sender.

28. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information is part of transactional account information that is associated with the public key of the sender in the computer database.

29. (Original) The method of claim 28, wherein the transactional account information comprises business process information.

30. (Original) The method of claim 28, wherein the transactional account information comprises a history of ledger transactions in the account.

31. (Original) The method of claim 28, wherein the account comprises a checking account.

32. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information is stored in

fields in records in a computer database.

33. (Original) The method of claim 32, wherein the records comprise an account file.
34. (Original) The method of claim 32, wherein the records further comprise a transactions file.
35. (Original) The method of claims 1, 2, 3, or 4, wherein the digital signature is derived within a hand-held device of the sender.
36. (Original) The method of claims 1, 2, 3, or 4, wherein the entity information comprises personal information of the sender.
37. (Original) The method of claims 1, 2, 3, or 4, wherein the function of the electronic message comprises applying a hashing algorithm to the electronic message.